AFFIDAVIT

I, Patrick Hanna, being duly sworn, depose and state as follows:

Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and currently assigned to the Burlington Resident Agency in Vermont. I have been an FBI Special Agent for 20 years. My duties as an FBI Special Agent include investigating violations of Title 18 of the United States Code as they pertain to corporate fraud, complex financial crimes, embezzlement, public corruption, money laundering and related white-collar crimes, as well as violent crimes and criminal enterprises. I have participated in investigations of criminal violations of various federal laws. I have executed search and arrest warrants, interviewed and interrogated subjects, witnesses, and victims, and conducted surveillance. In the course of these investigations, I have gained an understanding of current technology, to include computers and online accounts, cellular telephones and associated records and data, and have conducted analyses of the data related to such accounts and devices, for the purpose of solving and proving crimes.

2. I make this affidavit in support of an application for a search warrant for information associated with Apple ID sgumrukcu@yahoo.com stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Attachment A. Upon receipt of the information described in Attachment B, government-authorized persons will review that information to locate the items described in Attachment B.

3. On May 19, 2022, the federal grand jury sitting in Burlington, Vermont, charged Serhat Gumrukcu with conspiring with Berk Eratay and others between May 2017 and February 2018 to pay someone to murder Gregory Davis, whose body was discovered on January 7, 2018. On December 13, 2022, the grand jury returned an additional charge against Gumrukcu and Eratay, alleging that the two conspired between 2015 and 2018 to commit wire fraud by misrepresenting various relevant facts to Davis and Gregory Gac. As discussed below, there is probable cause to believe that Gumrukcu was involved in this murder-for-hire conspiracy, along with Eratay, Aron Ethridge, and Jerry Banks. Davis's murder involved the following federal crimes: kidnapping, in violation of 18 U.S.C. § 1201; murder to obstruct justice, in violation of 18 U.S.C. § 1512(a)(1); murder for hire, in violation of 18 U.S.C. § 1958; and wire fraud, in violation of 18 U.S.C. § 1343.

4. This case is being investigated by the FBI and the Vermont State Police (VSP). Since this affidavit is being submitted for the limited purpose of establishing probable cause to search data already in law enforcement's custody, I have not included details of every aspect of the investigation. Except as otherwise noted, the information contained in this affidavit is based

upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and my review of documents and records.

Probable Cause

5. On June 10, 2022, I obtained a search warrant for an Apple iPhone and an Apple MacBook Pro laptop seized from Serhat Gumrukcu on May 24, 2022. Currently, FBI forensic examiners have been unable to extract relevant data from these two devices but efforts remain ongoing. I have attached the affidavit in support of the application for that warrant and adopt that as probable cause to obtain and search the iCloud data. Exhibit 1. That affidavit and its attachments accurately reflect evidence developed at that time. Since then, I have learned additional facts. One aspect of the investigation that should be updated is my understanding of the use of two Google email accounts (muratsgumrukcu@gmail.com and murtagumrukcu@gmail.com) that appeared to be used by Murat Gumrukcu, Serhat Gumrukcu's brother. I have developed substantial evidence that Berk Eratay and/or Serhat Gumrukcu generated the emails supposedly from Murat Gumrukcu, who I have learned could not speak English fluently. This evidence, along with other evidence, supported the additional wire fraud conspiracy charge against Serhat Gumrukcu and Berk Eratay in the Second Superseding Indictment. Thus, at this time, Murat Gumrukcu may have not been involved in the murder plot. With this additional information, I incorporate the other information in Exhibit 1 and its attachments for purposes of this affidavit.

6. As described below, I believe that Gumrukcu used Apple iCloud services. Based on my training and experience, as well as conversations with FBI forensic experts, I believe that Gumrukcu used iCloud to store data, such as emails, text messages and other communication applications such as FaceTime and iMessages, that would also have been stored on his Apple phone and computer. Thus, I believe that there is probable cause to search the iCloud data for the same reasons that there was probable cause to search Gumrukcu's phone and computer.

Identification of iCloud Account

7. On July 27, 2022, a preservation request for the iCloud accounts of Serhat D. Gumrukcu, 310-590-8250 was sent to Apple, Inc. and receipt was confirmed by Apple, Inc. On January 31, 2023, an extension of preservation was sent to Apple, Inc. regarding Serhat D. Gumrukcu, 310-590-8250.

8. I reviewed records provided by Apple in response to a subpoena regarding Serhat D. Gumrukcu, 310-590-8250. The return outlined one account identifier associated with Serhat Gumrukcu listed as Apple ID "sgumrukcu@yahoo.com" and a DS ID of "1000916171". The account type is listed as "Full iCloud (iCloud+)". The day phone listed on the account is 1-310-590-8250 and the FaceTime/iMessage Phone number is listed as 1-310-590-8250. The name associated with the account is Serhat Gumrukcu with an address of 8581 Santa Monica Blvd #317, Ste 317, West Hollywood, California 90069-4120. The records showed the account as

active and the creation date of October 15, 2011. Based on my investigation, these identifiers match the Serhat Gumrukcu under investigation.

9. As noted above, the FBI was unable to extract most of the content from the iPhone seized from Gumrukcu in May 2022. The FBI was able, however, to extract some data from the phone. The extracted data did not include the typical information available to an iPhone user, but it did include certain information including account information and log information that indicates that Gumrukcu used iCloud and the iCloud account described above in paragraph 8 as early as 2013.

Background Concerning Apple[1]

10. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

11. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

12. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

13. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

14. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means

of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

15. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

16. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

17. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on

iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

18. As noted above, I believe that information in the iCloud account may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element.

19. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

20. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

21. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

Conclusion

22. Based on the forgoing, I request that the Court issue the proposed search warrant.

23. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Attested to by the applicant in accordance with the requirements of Federal Rule of Criminal Procedure 4.1 by Zoom call on February 24, 2023.

/s/ Geoffrey W. Crawford

Honorable Geoffrey W. Crawford
United States District Judge